CLAIMS

What is claimed is:

1. A method for remote mirroring of network traffic, the method comprising:
receiving a data packet to be remotely mirrored by an entry device pre-configured with a destination Internet Protocol (IP) address to which to mirror the data packet;
generating and adding an IP header to IP encapsulate the data packet, wherein the IP header includes the destination IP address; and
forwarding the IP-encapsulated packet to an exit device associated with the destination IP address.

2. The method of claim 1, further comprising:
determining a media access control (MAC) address associated with the destination IP address;
generating and adding a MAC header to the IP-encapsulated packet to form a MAC data frame, wherein the MAC header includes the MAC address in a destination field; and
transmitting the MAC data frame to communicate the IP-encapsulated packet across a layer 2 domain.

3. The method of claim 2, wherein determining the MAC address comprises:
determining if a mapping of the destination IP address to the MAC address is stored in an address resolution protocol (ARP) cache;
if so, then retrieving the MAC address from the ARP cache; and
if not, then broadcasting an ARP request with the destination IP address and receiving an ARP reply with the MAC address.

4. The method of claim 2, wherein the IP-encapsulated packet is communicated across at least one intermediate layer 2 domain.

5. The method of claim 1, further comprising:
receiving the IP-encapsulated packet by the exit device; and
removing the IP header to de-encapsulate the packet.

6. The method of claim 1, wherein the remote mirroring preserves an original format of the data packet.

7. The method of claim 1, further comprising:
pre-configuring the entry device to mirror data packets from at least one specified port of the entry device.

8. The method of claim 1, further comprising:
pre-configuring the entry device to mirror data packets which include a VLAN tag with at least one specified VLAN identifier.

9. The method of claim 1, further comprising:
pre-configuring the entry device to mirror data packets which include MAC addresses that matches at least one entry in a MAC look-up table.

10. The method of claim 1, further comprising:
pre-configuring the entry device to mirror data packets which include IP addresses that matches at least one entry in an IP hash table.

11. The method of claim 1, further comprising:
pre-configuring the entry device to mirror data packets which include an IP destination address that matches at least one specified subnet entry in a best matching prefix (BMP) table.

12. The method of claim 1, further comprising:
pre-configuring the entry device to mirror data packets matching at least one access control list (ACL) entry.

13. The method of claim 1, further comprising:
configuring the entry device in a best effort mirroring mode to reduce head-of-line blocking.

14. The method of claim 1, further comprising:

configuring the entry device in a lossless mirroring mode to assure completeness of mirrored traffic.

15. The method of claim 1, further comprising:
truncating the data packet to reduce a size of the IP-encapsulated packet prior to forwarding thereof.

16. The method of claim 1, further comprising:
compressing at least a portion of the data packet to reduce a size of the IP-encapsulated packet prior to forwarding thereof.

17. The method of claim 1, further comprising:
encrypting at least a portion of the data packet to provide a level of security prior to forwarding the IP-encapsulated packet.

18. A networking device comprising:
a plurality of ports for receiving and transmitting packets therefrom;
a switching/routing engine coupled to the ports for transferring the packets therebetween; and
a remote mirroring engine configured to detect packets from a specified mirror source, IP-encapsulate the detected packets, and forward the IP-encapsulated packets to an IP destination by way of at least one of the ports.

19. The networking device of claim 18, wherein the specified mirror source comprises at least one of said ports.

20. The networking device of claim 18, wherein the specified mirror source comprises at least one specified VLAN.

21. The networking device of claim 18, wherein the specified mirror source comprises those packets matching entries in a look-up table.

22. The networking device of claim 18, wherein the specified mirror source comprises at least one specified subnet.

23. The networking device of claim 18, wherein the specified mirror source comprises those packets matching entries in an access control list.

24. The networking device of claim 18, wherein the device includes a best effort mirroring mode to reduce head-of-line blocking.

25. The networking device of claim 18, wherein the device includes a lossless mirroring mode to assure completeness of mirrored traffic.

26. The networking device of claim 18, wherein the device truncates the data packet to result in a size reduction of the IP-encapsulated packet prior to forwarding thereof.

27. The networking device of claim 18, wherein the device compresses at least a portion of the data packet to result in a size reduction of the IP-encapsulated packet prior to forwarding thereof.

28. The networking device of claim 18, wherein the device encrypts at least a portion of the data packet to provide a level of security prior to forwarding the IP-encapsulated packet.

29. An apparatus for remote mirroring of network traffic, the method comprising:

means for receiving a data packet to be remotely mirrored by an entry device pre-configured with a destination Internet Protocol (IP) address to which to mirror the data packet;

means for generating and adding an IP header to IP encapsulate the data packet, wherein the IP header includes the destination IP address; and means for forwarding the IP-encapsulated packet to an exit device associated with the destination IP address.